VOICEMAIL FRAUD

In recent months, there have been news reports in the media about voicemail customers whose voicemail mailboxes have been compromised. The primary method for these hackers to successfully compromise mailbox security occurred when customers had not initialized their mailboxes, had not changed their temporary passwords or had selected passwords that were easy to guess.

Once the mailbox had been compromised, the hackers would change the customers greeting to accept charges for international or long distance calls resulting in large long distance charges to the customer.

We would like to take this opportunity to remind you of some easy safety tips that will assist in the security of your mailboxes. For your security, you should change your temporary password immediately, even if you are not yet using your mailbox.

- When choosing a password, do not use your telephone or mailbox number (or any part of the telephone or mailbox number) as part of the password.
- Do not repeat digits (e.g. 444444), do not use sequential digits (e.g. 123456) and do not use easily identifiable numbers (e.g. zip code, street address, etc).
- Treat your password as you would your ATM pin. Select a password of at least six digits, up to a maximum of 13.
- For added security, you should change your password periodically and check your greetings to make sure they have not been changed.

By following these simple security recommendations, you can reduce the chances of this type of fraud from occurring. Please share this information within your organization as you deem appropriate and necessary in order to reach everyone with voicemail password access.

If you have any questions, please contact your local SBC representative.